

# Firmware Analysis of NetBotz (APC - Schneider Electric) Rack Monitor 570/550/450 and Wall Monitor 455/355 - 4.5.3

March 30, 2018

## Meta Data

HID	NetBotz (APC - Schneider Electric) Rack Monitor 570/550/450 and Wall Monitor 455/355 - 4.5.3
Device Name	Rack Monitor 570/550/450 and Wall Monitor 455/355
Vendor	NetBotz (APC - Schneider Electric)
Device Class	DVR
Version	4.5.3
Release Date	2016-11-02
Size	21.58 MiB (22,632,490 bytes)

## Analysis

### base64decoder

Time of Analysis	2018-03-29 13:02:26
Plugin Version	0.1.2
Summary	

### cpu architecture

Time of Analysis	2018-03-29 13:06:10
Plugin Version	0.3.1
Summary	PPC (M)

### crypto material

Time of Analysis	2018-03-29 13:02:05
Plugin Version	0.5
Summary	

## exploit mitigations

Time of Analysis	2018-03-29 13:06:14
Plugin Version	0.1.1
Summary	

## file hashes

Time of Analysis	2018-03-29 13:06:19
Plugin Version	1.0
imphash	None
md5	aff3ed2821d4a3c0e1cb0a56c0048393
ripemd160	450c7e078958fd4b58214005acb44a7fc36c6f58
sha1	164eb4233b78da456232c082dcdf5a0dd4021919
sha256	26ef025078abda69d2c3de06e27142a6db1a6385bd2524ce4976211570264a39
sha512	
da38955f0df1be8e9713967c6d2e5d5d27ca1bd421e96f9159ab802b4586d8b4b1fe62dbb2092ed4b8521986d25724e0a54e308	
ssdeep	
393216:JCWk8T1ykEFKvGf+/9vFmYS678jcZOzzyHGUPccDuHiWcCWTi0PlhHa:a8TokvQ+IU2tOzQPuCWyTXIl	
whirlpool	
2517d24d06ac652e06bfb32b4b1a70e899a6b0a48963e9f2262204a3e303b80f6e44c66027781ed412557df4bf64bd3b788190	

## file type

Time of Analysis	2018-03-29 13:05:56
Plugin Version	1.0
File Type	uImage header, header size: 64 bytes, header CRC: 0x759DDD, created: Fri Sep 30 15:50:56 2016, image size: 22632426 bytes, Data Address: 0x0, Entry Point: 0x0, data CRC: 0x3E9EC215, OS: Linux, CPU: PowerPC, image type: RAMDisk Image, compression type: gzip, image name: "V4.5.3.20160930_1058"
MIME	firmware/u-boot
Summary	firmware/u-boot

## init systems

Time of Analysis	2018-03-29 13:05:59
Plugin Version	0.4.1
Summary	

## ip and uri finder

Time of Analysis	2018-03-29 13:01:59
Plugin Version	0.4.1
IPs v4	list is empty

IPs v6	83:: ::9F ::a ::2D2 2::7 :: 7:: C:: 5:: 1:: ::B F:: ::3 ::E 8:: 3::b 02:: E2:: c:: 6::E ::F ::c 6:: 4:: 0::A ::bF ::4 B:: ::e ::8 61::5 ::d E:: ::5 9::D3 a:: A:: D::
URIs	list is empty
Summary	83:: ::9F ::a ::2D2 2::7 :: 7:: C::

5::
1::
::B
F::
::3
::E
8::
3::b
02::
E2::
c::
6::E
::F
::c
6::
4::
0::A
::bF
::4
B::
::e
::8
61::5
::d
E::
::5
9::D3
a::
A::
D::

### software components

Time of Analysis	2018-03-29 13:05:50
Plugin Version	0.3
Summary	

### printable strings

Time of Analysis	2018-03-29 13:05:39
Plugin Version	0.2
string count	45253

### users and passwords

Time of Analysis	2018-03-29 13:05:47
Plugin Version	0.4
Summary	

### string evaluator

Time of Analysis	2018-03-29 13:06:08
Plugin Version	0.2
string count	45253

### unpacker

Time of Analysis	2018-03-29 13:01:18
Plugin Version	0.1
Plugin	Uboot
Extracted	2
Output:	
Output	
size packed -> unpacked	21.57 MiB -> 21.58 MiB
entropy	0.89
Summary	no data lost

### malware scanner

Time of Analysis	2018-03-29 13:05:52
Plugin Version	0.3
MD5	aff3ed2821d4a3c0e1cb0a56c0048393
System Version	0.2.6
Scanners Number	1
Positives	0
Scanners	ClamAV
Scanns	ClamAV :: version:ClamAV 0.99.4/24430/Thu Mar 29 06:23:16 2018 ClamAV :: result:clean ClamAV :: detected:False
Summary	